Draft new Recommendation Y.QKDN-iwfr

Quantum key distribution networks - interworking framework

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN_iwfr specifies framework of interworking QKDNs.

Keywords

QKD, QKDN (QKD network), interworking

Table of Contents

Draft new Recommendation Y.QKDN-iwfr

Quantum key distribution networks - interworking framework

Editor's note – The initial draft was created by compiling from multiple proposals. Contributions are invited to improve it at the next meeting.

1. Scope

This Recommendation specifies a framework for interworking QKDNs.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Cor.1 (2020), *Overview on networks supporting quantum key distribution*.

[ITU-T Y.3801] Recommendation ITU-T 3801 (2020) *Functional requirements for quantum key distribution network.*

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the quantum key distribution network*.

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Key management for quantum key distribution Networks*

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Control and* Management for Quantum Key Distribution Networks.

[ITU-T Y.QKDN_BM] Draft Recommendation ITU-T Y.QKDN_BM: “Quantum Key Distribution Networks - Business role-based models”

3. Definitions

3.1. Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **key manager (KM)** [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.2 **quantum key distribution (QKD)** [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.3 **quantum key distribution link (QKD link)** [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.4 **quantum key distribution module (QKD module)** [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.5 **quantum key distribution network (QKDN)** [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.1.6 **quantum key distribution network controller (QKDN controller)** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.7 **quantum key distribution network manager (QKDN manager)** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.8 **quantum key distribution node (QKD node)** [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.2. Terms defined in this Recommendation

This Recommendation defines no term.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
IT-secure	Information-theoretically secure
KM	Key manager
OTP	One-time pad encryption
PKI	Public Key infrastructure
QKD	Quantum Key Distribution
QKDN	QKD Network

5. Conventions

None.

6. Overview of interworking QKDNs

Editor's note - Interworking categorization and priorities of study can be indicated in a table. It is for further study at the next meeting.

Quantum key distribution network (QKDN) is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other.

The functional requirements and architecture of single QKDN are specified based on the functional requirements of QKDN in [ITU-T Y.3801], functional architecture and operational procedures of QKDN in [ITU-T Y.3802].

This Recommendation will consider the following aspects for interworking QKDNs.

1) Interworking between QKDNs supported by different QKDN providers.

NOTE 1 - QKDN provider is specified in [draft ITU-T Y.QKDN_BM].

2) Interworking between QKDNs with different technologies.

Different technologies can be used in QKDNs such as:

- Key relay encryption methods (i.e. OTP, AES etc.)
- Key relay schemes (i.e. case 1 and case 2 which are specified in [ITU-T Y.3800])
- Key relay alternatives (i.e. XORs uniformly processed at destination node etc. which are specified in [ITU-T Y.3803])
- Configurations of QKDN controller (i.e. centralized QKDN or distributed QKDN which are specified in [ITU-T Y.3802]
- Protocols in the key management layer, the QKDN control layer and the QKDN management layer.

NOTE 2 – Details of protocols are outside the scope of this Recommendation.

7. Interworking of QKDNs among multiple QKDN providers

In case that different QKDN providers supply QKD key to each end’s cryptographic application in user network, their QKDNs should be interworked. Figure 1 shows a conceptual interworking configuration between QKDN providers.

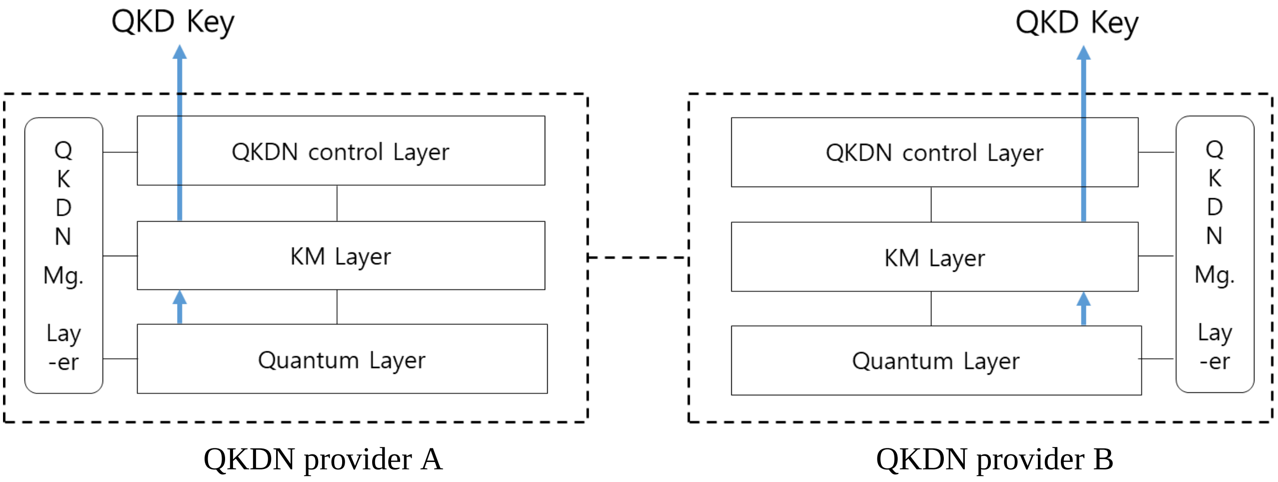
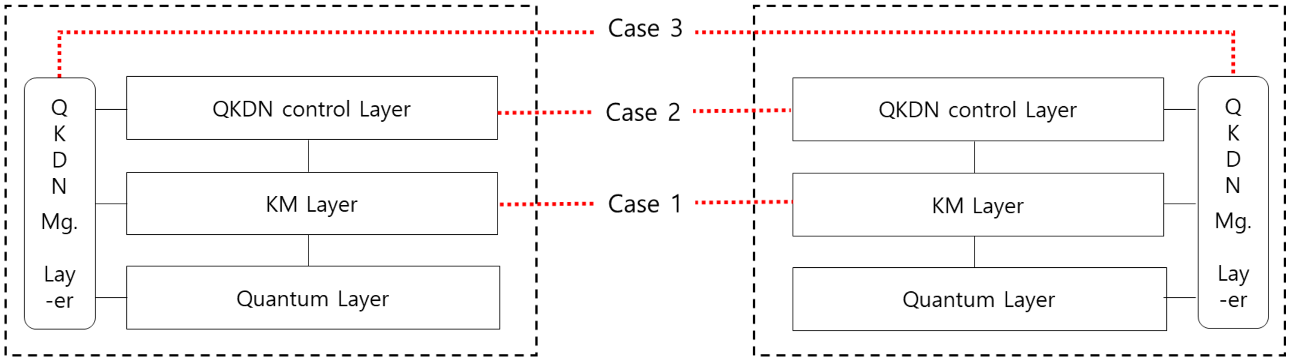


Figure 1. conceptual interworking between QKDNs supported by different QKDN providers

For the purpose of practical aspects, three types of interworking configurations should be considered at least.



QKDN provider A QKDN provider B

Figure 2. practical interworking configurations of interworking QKDNs among multiple QKDN providers.

Case 1) KM layer interworking; When QKD key relays between QKDN operators through KM layer, relative information for this purpose should be communicated, such as key ID, QKD module ID, key generation date, etc.

Case 2) QKDN control layer interworking; QKDN control information should be shared between QKDN operators through QKDN control layer, such as routing control, session control, authentication and authorization control and QoS policy control, etc.

Case 3) QKDN management layer interworking; QKDN management information should be shared between QKDN operators through QKDN management layer, such as fault, configuration, accouting, performance and security management.

NOTE - Quantum layer interworking is out of scope in the document.

Figure 3 illustrates a practical configuration of interworking QKDNs among multiple QKDN providers.

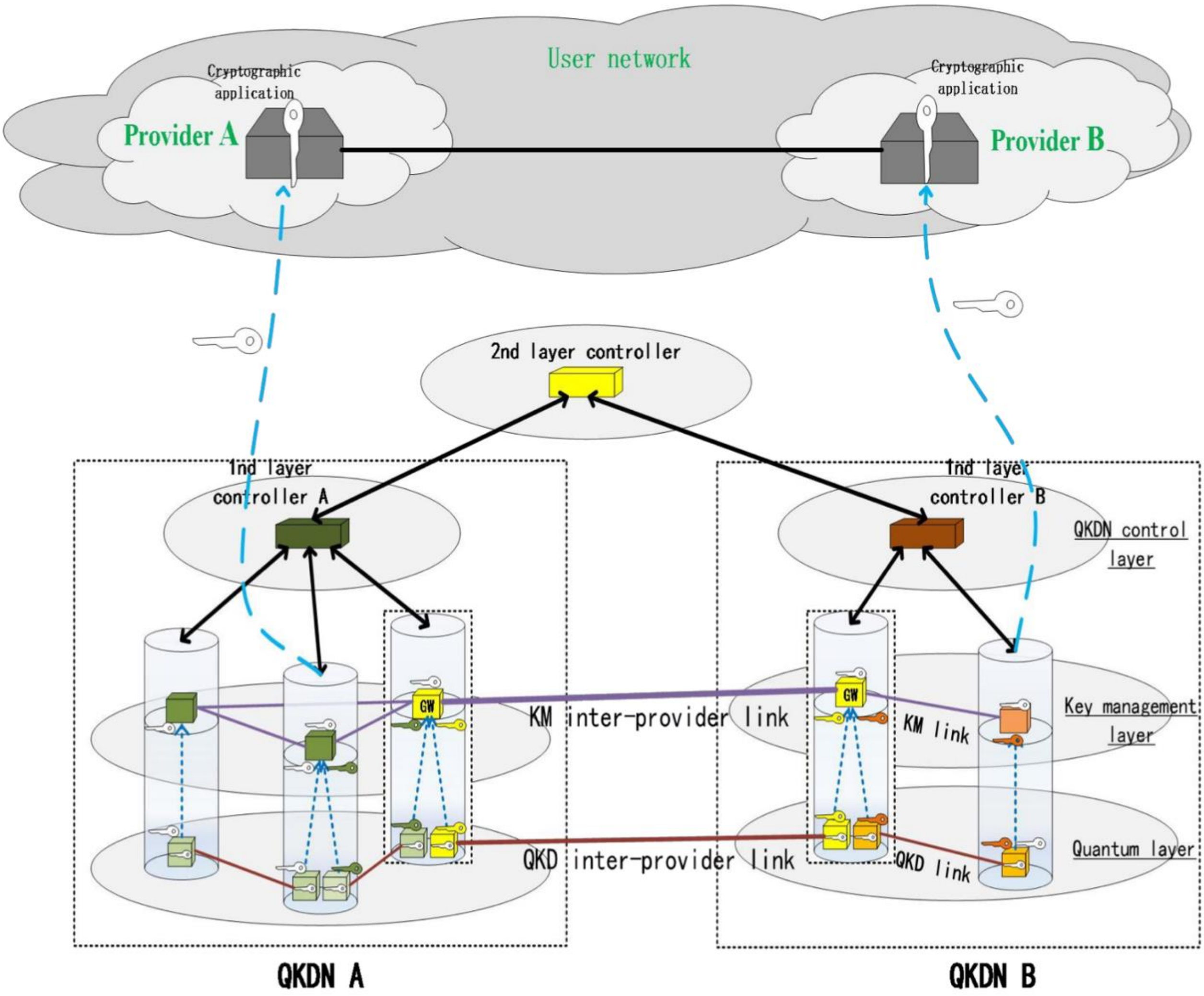


Figure 3 - A practical configuration of interworking QKDNs among multiple QKDN providers

The QKDN A and the QKDN B may consist of different QKDN providers. Different technologies can be used in the QKDN A and the QKDN B such as:

-Configurations of QKDN controller (i.e. centralized QKDN or distributed QKDN which are specified in [ITU-T Y.3802].

8. Interworking of QKDNs with different technologies

Figure 4 illustrates a practical configuration of interworking QKDNs with different technologies.

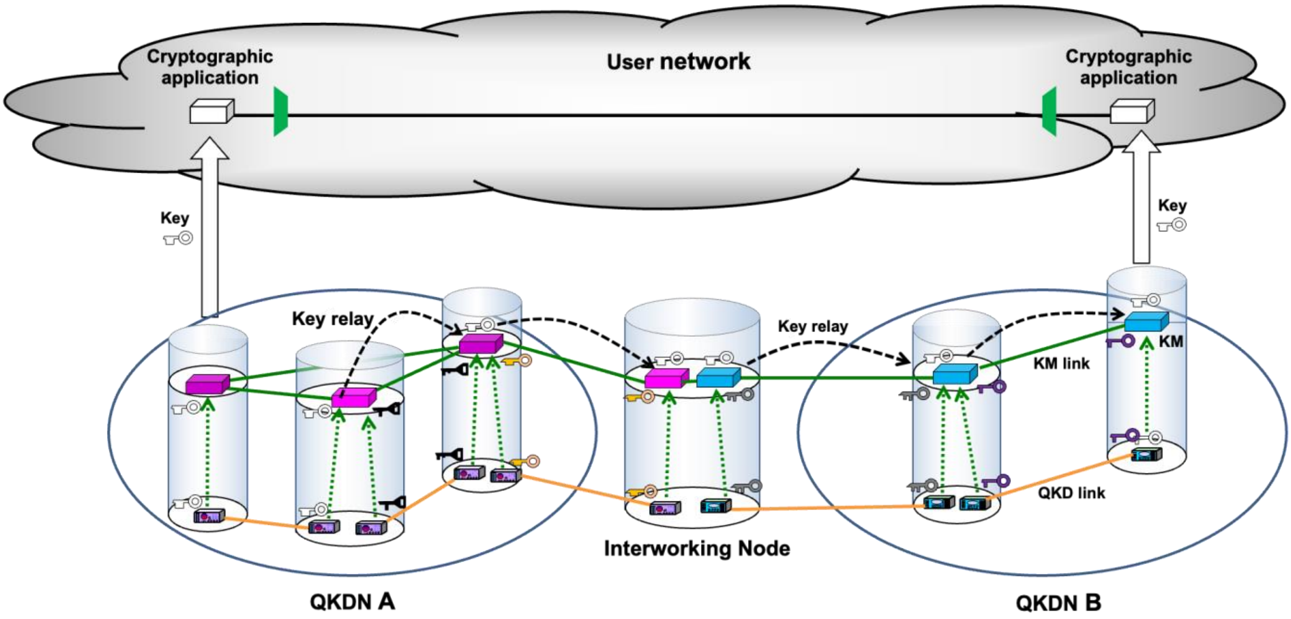


Figure 4 – A practical configuration of interworking QKDNs with different technologies

Figure 5 illustrates a conceptual model of interworking QKDNs with different technologies.

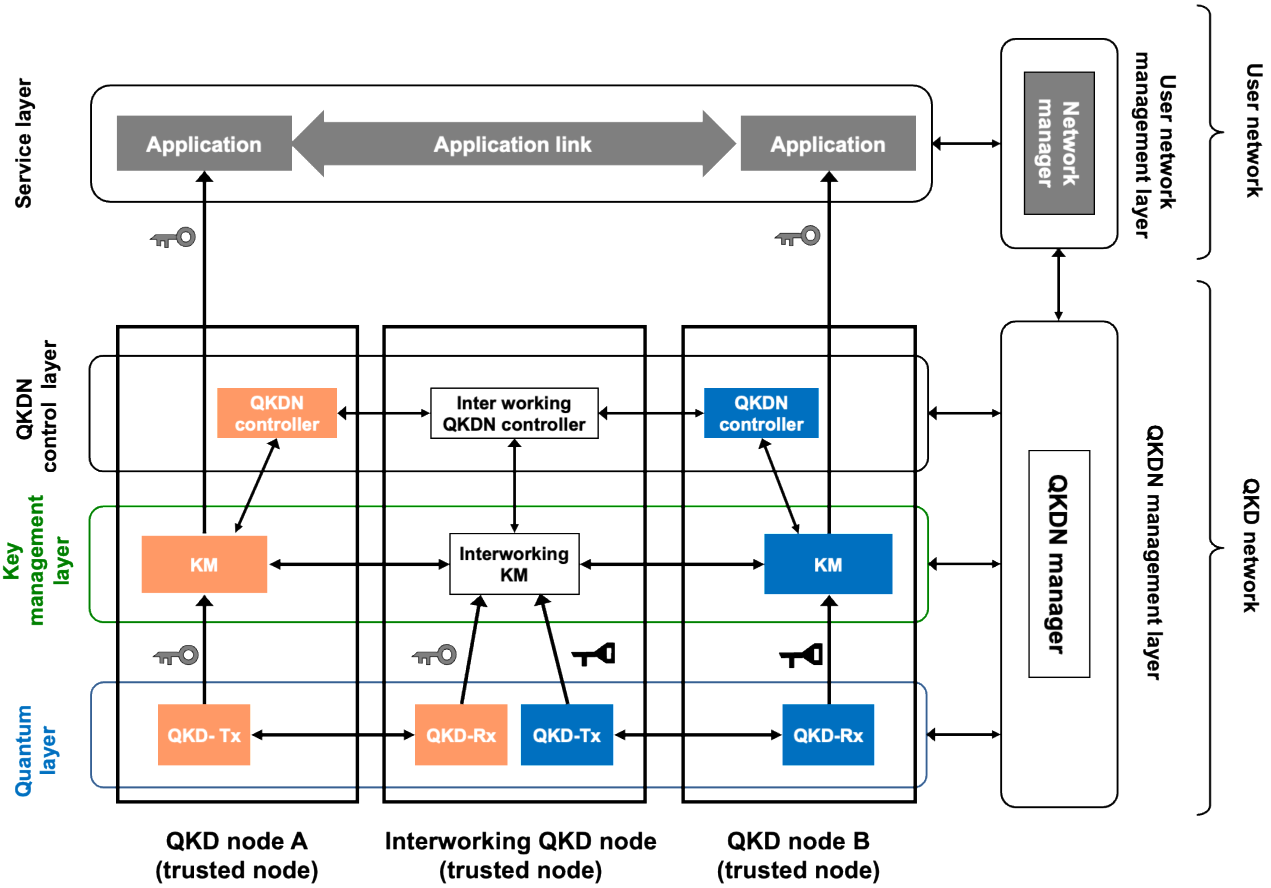


Figure 5 - A conceptual model of interworking QKDNs with different technologies.

In this conceptual model, the QKDN A and the QKDN B are connected via the interworking QKD node. The interworking QKD node performs interworking functions between QKDNs which use different technologies provided by different vendors.

NOTE - Connecting between QKD modules in the QKDN A and the QKDN B is outside the scope of this Recommendation because QKD protocols on QKD links are not well standardized.

9. Security consideration

To be added.

Appendix I

Title of Appendix I

(This appendix does not form an integral part of this Recommendation.)

Annex A

A.1 justification for proposed draft new Recommendation Y.QKDN_iwfr

Question:	16/13	**Proposed new ITU-T Recommendation**	Virtual, 5-16 July 2021
Reference and title:	Draft Recommendation Y.QKDN-iwfr "Quantum key distribution networks - interworking framework"		
Base text:	SG13-TD604/WP3	**Timing:**	2023-Q1
Editor(s):	Zhao Yongli, BUPT China Yasuhiro FUJIYOSHI, Toshiba corporation Japan Hyungsoo Kim, KT Korea (Rep. of) Taesang Choi, ETRI Korea (Rep. of)	**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Recommendation specifies a framework for interworking QKDNs.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

Quantum key distribution network (QKDN) is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other.

The functional requirements and architecture of single QKDN are specified based on the functional requirements of QKDN in [ITU-T Y.3801], functional architecture and operational procedures of QKDN in [ITU-T Y.3802]. This recommendation is to specify a framework for interworking QKDNs. Security considerations are mentioned when it is directly related to the security of keys.

This Recommendation will consider the following aspects for interworking QKDNs.

1) Interworking between QKDNs supported by different QKDN providers.

NOTE – QKDN provider is specified in [draft ITU-T Y.QKDN_BM].

2) Interworking between QKDNs with different technologies.

Different technologies can be used in QKDNs such as:

- Key relay encryption methods (i.e. OTP, AES etc.)
- Key relay schemes (i.e. case 1 and case 2 which are specified in [ITU-T Y.3800])
- Key relay alternatives (i.e. XORs uniformly processed at destination node etc. which are specified in [ITU-T Y.3803])
- Configurations of QKDN controller (i.e. centralized QKDN or distributed QKDN which are specified in [ITU-T Y.3802]

- Protocols in the key management layer, the QKDN control layer and the QKDN management layer.

NOTE – Details of protocols is outside the scope of this Recommendation.

Relations to ITU-T Recommendations or to other standards (approved or under development):

This WI will refer to the QKDN Recommendations such as ITU-T Recommendation Y.3800, Y.3801, Y.3802, Y.3803, Y.3804 and X.1710.

This work item will collaborate with FG and other SDOs such as FG-QIT4N and ETSI ISG-QKD.

The proposed new WI will be studied in a harmonious manner with existing and ongoing works in ITU-T and other SDOs but there are no duplications identified so far.

Liaisons with other study groups or with other standards bodies:

ITU-T SG11, SG17, FG-QIT4N, ETSI ISG QKD

Supporting members that are committing to contributing actively to the work item:

BUPT, CAS Quantum Network, QuantumCTek, CAICT, NICT, NEC, Toshiba, ETRI, KT, SKT

Bibliography